CLAIMS
In the Claims:

Please cancel claims 1-24.

Please add the following new claims:

25. A memory device comprising:

a main memory array;

an internal processor to execute programming code; and

a hidden storage area connected to the main memory array;

wherein the programming code prevents access to the hidden storage area without a valid password.

26. The memory device of claim 25, wherein the main memory array is a non-volatile writable memory array.

27. The memory device of claim 26, wherein the non-volatile writable memory array includes at least one of a flash memory array, a battery backed memory array, and a polymer memory array.

28. The memory device of claim 25, wherein the hidden storage area comprises one or more hidden memory banks.

29. The memory device of claim 28, wherein the hidden memory banks are divided into one or more user spaces and a password space containing one or more stored valid reference passwords.

30. The memory device of claim 29, wherein the valid password allows accesses to only one of the user spaces.

31. The memory device of claim 28, wherein the hidden memory banks include a swap space to copy data between the hidden memory banks without exposing the data in the hidden memory banks.

32. The memory device of claim 28, wherein the hidden storage area further comprises a bank selector to select a hidden memory bank.

33. The memory device of claim 28, wherein the hidden storage area further comprises an output bus gate to prevent access to the hidden memory banks.

34. The memory device of claim 33, wherein the hidden storage area further comprises an address decoder to open the output bus gate when provided the valid password.

35. The memory device of claim 33, wherein the hidden storage area further comprises an address decoder to open the output bus gate when provided a valid memory address within the hidden memory banks.

36. The memory device of claim 35, wherein the valid memory address is provided by a host.

37. The memory device of claim 25, wherein the hidden storage area further comprises a valid password indicator to indicate a password has been verified by an internal processor.

38. The memory device of claim 25, wherein the memory device further comprises a bad password counter, to count the number of times the internal processor is unable to verify the password.

39. The memory device of claim 25, wherein the memory device is connected to a bad password counter, to count the number of times the internal processor is unable to verify the password.

40. A method, comprising:

storing one or more valid passwords in a hidden memory area;

receiving a password at an internal processor connected to the hidden memory area; and

executing programming code to verify the password against a valid reference password stored within the hidden memory area.

41. The method of claim 40, further comprising permitting access to read from the hidden memory area if the password is verified.

42. The method of claim 40, further comprising permitting access to write to the hidden memory area if the password is verified.

43. The method of claim 40, further comprising permitting access to write to the hidden memory area if a valid address in the hidden memory area is provided.

44. The method of claim 40, further comprising dividing the hidden memory area into one or more user spaces, a password space, and a swap space.

45. The method of claim 40, further comprising writing a recovery password that allows a bad password counter to be reset.

46. The method of claim 40, further comprising writing a system administrator password that allows hidden memory area contents to be reset.

47. The method of claim 40, further comprising writing a system administrator password that allows a recovery password to be reset.

48. The method of claim 40, further comprising writing a system administrator password that allows a bad password counter to be reset.

49. A computer readable medium having stored thereon a plurality of instructions, said plurality of instructions when executed by a computer, cause said computer to perform:
storing one or more valid passwords in a hidden memory area;
receiving a password at an internal processor connected to the hidden memory area; and
executing programming code to verify the password against a valid reference password stored within the hidden memory area.

50. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further perform a read from the hidden memory area if the password is verified.

51. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further

perform a write to the hidden memory area if the password is verified; and a valid address in the hidden memory area is provided.

52. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further perform dividing the hidden memory area into one or more user spaces, a password space, and a swap space.

53. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further perform writing a recovery password that allows a bad password counter to be reset.

54. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further perform writing a system administrator password that allows hidden memory area content to be reset.

55. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further perform writing a system administrator password that allows a recovery password to be reset.

56. The computer-readable medium of claim 49 having stored thereon additional instructions, said additional instructions when executed by a computer, cause said computer to further perform writing a system administrator password that allows a bad password counter to be reset.

57. A system comprising:

a wireless communications transceiver; and

a memory device coupled to the wireless communications transceiver, including

a main memory array;

an internal processor to execute programming code; and

a hidden storage area connected to the main memory array;

wherein the programming code prevents access to the hidden storage area without a valid password.

58. The memory device of claim 57, wherein the main memory array is a non-volatile writable memory array.

59. The memory device of claim 58, wherein the non-volatile writable memory array includes at least one of a flash memory array, a battery backed memory array, and a polymer memory array.

60. The memory device of claim 57, wherein the hidden storage area comprises one or more hidden memory banks.